THE DEPARTMENT OF DEFENSE INFORMATION NETWORK (DODIN): A STUDY OF CURRENT CYBER THREATS AND BEST PRACTICES FOR NETWORK SECURITY

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

SCOTT M. BAILEY, MAJOR, U.S. ARMY
B.S., Ball State University, Muncie, Indiana, 2001

Fort Leavenworth, Kansas
2016

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
10-06-2016	Master's Thesis	AUG 2015 – JUNE 2016

4. TITLE AND SUBTITLE The Department of Defense Information Network (DODIN): A Study of Current Cyber Threats and Best Practices for Network Security	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) MAJ Scott M. Bailey	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Department of Defense Information Network (DODIN) is being threatened by state actors, non-state actors, and continuous hacking and cyber-attacks. These threats against the network come in a variety of forms; physical attacks from radio jamming, logical cyber threats from hacking, or a combination of both physical and logical attacks. Each year the number of hacking attacks is increasing. Corporations like Symantec publish annual reports on cyber threats and provide tips for best practices to defend against cyber-attacks. Military doctrine provides tactics, techniques and procedures for countering electronic warfare attacks. The MITRE Corporation maintains the Common Vulnerabilities and Exposures (CVE) List of defined viruses and makes the information publicly available so that security professionals can collaborate in building more secure networks. A literature review of recent hacking attacks, physical cyber threats, and mixed attacks provides historical context of the current cyber threat. Review of best practices for network security and protection against electronic warfare provides tools for Signal Officers to implement in their networks. Finally by analyzing the Common Vulnerabilities and Exposures (CVE) List for virus trends the researcher provides a current benchmark of the security threats through January 2016 in order to plan for future network defense measures.

15. SUBJECT TERMS
Cyber, network security, electronic warfare, Department of Defense Information Network, DODIN, common vulnerabilities and exposures, CVE List, Signal Corps

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	69	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Scott M. Bailey

Thesis Title: The Department of Defense Information Network (DODIN): A Study of Current Cyber Threats and Best Practices for Network Security

Approved by:

____, Thesis Committee Chair
Clay Easterling, M.B.A.

____, Member
MAJ Kenneth C. Rich, Ph.D.

____, Member
Matthew W. Broaddus, M.A.

Accepted this 10th day of June 2016 by:

____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE DEPARTMENT OF DEFENSE INFORMATION NETWORK (DODIN): A STUDY OF CURRENT CYBER THREATS AND BEST PRACTICES FOR NETWORK SECURITY, by Major Scott M. Bailey, 69 pages.

The Department of Defense Information Network (DODIN) is being threatened by state actors, non-state actors, and continuous hacking and cyber-attacks. These threats against the network come in a variety of forms; physical attacks from radio jamming, logical cyber threats from hacking, or a combination of both physical and logical attacks. Each year the number of hacking attacks is increasing. Corporations like Symantec publish annual reports on cyber threats and provide tips for best practices to defend against cyber-attacks. Military doctrine provides tactics, techniques and procedures for countering electronic warfare attacks. The MITRE Corporation maintains the Common Vulnerabilities and Exposures (CVE) List of defined viruses and makes the information publicly available so that security professionals can collaborate in building more secure networks. A literature review of recent hacking attacks, physical cyber threats, and mixed attacks provides historical context of the current cyber threat. Review of best practices for network security and protection against electronic warfare provides tools for Signal Officers to implement in their networks. Finally, by analyzing the Common Vulnerabilities and Exposures (CVE) List for virus trends the researcher provides a current benchmark of the security threats through January 2016 in order to plan for future network defense measures.

ACKNOWLEDGMENTS

I would like to thank Mr. Matthew Broaddus for his continued mentorship and guidance throughout this academic year at the Command and General Staff College. His advice and extremely positive attitude have encouraged me to stay motivated throughout this research project. I would also like to thank my committee chairperson, Mr. Clay Easterling. His expertise and knowledge of the research process have been instrumental in the completion of this study. Thank you to Major Kenneth Rich who provided much appreciated guidance on research methods and references. Without the assistance of the entire committee this project would not have been possible. I would like to thank my parents, Mike and Kathy Bailey, for their love and support throughout my lifetime; we miss you dad. Thanks to my sister, Molly, for her continued love and support. Most of all, thank you to my children for inspiring me, and thank you to my wife to be, Gemma; your love and support give me strength every day.

TABLE OF CONTENTS

ACRONYMS

A2AD	Anti-Access and Area-Denial
ASAT	Anti-Satellite
BBC	British Broadcasting Corporation
C2	Command and Control
CEMA	Cyber and Electromagnetic Activities
CIA	Central Intelligence Agency
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DoD	Department of Defense
DODIN	Department of Defense Information Network.
DSSS	Direct Sequence Spread Spectrum
EW	Electronic Warfare
FHSS	Frequency-Hopping Spread Spectrum
FLOT	Forward Line of Own Troops
GCHQ	Government Communications Headquarters
GPS	Global Positioning System
ISIL	Islamic State in Iraq and the Levant
NATO	North Atlantic Treaty Organization
NPR	National Public Radio
NSA	National Security Agency
OPM	Office of Personnel Management
UWB	Ultra-Wide Band
WSN	Wireless Sensor Network

ILLUSTRATIONS

TABLES

Page

CHAPTER 1

INTRODUCTION

In April 2015 the Department of Defense (DoD) released *The Department of Defense Cyber Strategy* which outlined three primary cyber missions for the Defense Department:

> First, DoD must defend its own networks, systems, and information. . . . For its second mission, DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence. . . . Third, if directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans. (Carter 2015, 4-5)

The leaders of the Signal Corps are responsible for defending the networks, systems, and information which they manage as part of the Department of Defense Information Network (DODIN). The 2015 DoD Cyber Strategy also outlined the key cyber threats to the United States. These threats were characterized as originating from state actors like Russia, China, Iran, and North Korea; originating from non-state actors like the Islamic State in Iraq and the Levant (ISIL); and characterized as malware created for the proliferation of malicious code or software which could be used by nation states, non-state actors, or individual actors (Carter 2015, 9-10). The Department of Defense has focused its efforts and resources to defend cyberspace. The United States Army Cyber Center of Excellence has responded to the threat by outlining its science and technology objective capabilities for Force 2025 and beyond. In order to continue to make progress towards the defense and security of our vital communication networks the Department of Defense must understand the current operational environment, visualize the capabilities needed, and describe our operational approach. Conducting effective cyberspace and electronic warfare operations will continue to be critical mission for the Department of Defense. Members of the U.S. Army Signal Corps will focus on operating and maintaining the Department of Defense Information Network. Ultimately the Department of Defense must be able to safeguard from cyber-attacks, and provide support to military operations required to defend against future threats.

Introduction

In order to protect the Department of Defense Information Network communications professionals must first understand the threats and possible countermeasures to those threats. Increasing resiliency and improving cybersecurity must be a priority in order to conduct space and cyber electromagnetic operations and maintain communications (ARCIC 2016). These improved capabilities will assist in assuring freedom of operation in a communications contested environment. Some have reported that Electronic Warfare (EW) and cyber-attacks were carried out by Russia against the Ukraine beginning in March 2014 (Wiser 2015, 2). When a nation state actively uses electronic warfare and cyber-attacks against another sovereign nation it will immediately get the attention of the rest of the international community. Others have alerted the international community to the growing need to understand and develop countermeasures against electronic warfare (Gould 2015, 1). These kinds of attacks vary greatly in type and sophistication and countermeasures for this type of threat will need to be equally robust in order to provide protection against the wide range of possible threats.

Protecting the Department of Defense Information Network is of particular interest to the researcher because of his background as a Signal Officer. Other scholars and practitioners also share this common interest of providing secure communications for the Department of Defense and will possibly benefit from this research. The analysis of the Common Vulnerabilities and Exposures (CVE) List could be particularly useful to other network security professionals and researchers. This research contributes to ongoing research in the field of information technology, communications security, and software weakness types.

Background of the Study

Since 2007 cyber-attacks and electronic warfare incidents have taken place which have alarmed the international community to seriousness of this threat. Hacking attacks such as the denial of service attacks which occurred in Estonia in 2007 and Georgia in 2008 have proven to be effective in crippling computer infrastructure. The Stuxnet virus inflicted severe damage to Iranian nuclear infrastructure in June of 2010. Saudi Aramco fell victim to the Shamoon virus in August of 2012 which destroyed countless hard drives in the facility. Also in September of 2012 six U.S. banks were reportedly attacked by Iran in extreme denial of service attacks (Dev 2015, 394). Physical threats from China's development of the kinetic anti-satellite weapon have proven the possibility to conduct precision attacks on objects in space. GPS jamming continues to be of concern, and radio jamming techniques continue to improve. This broad overview regarding the security of command and control networks highlights the need for a thorough protection plan and development of countermeasures to defeat cyber-attacks and electronic warfare.

Several key researchers and organizations have contributed greatly to the information available for software weakness types, network security, and threats to the Department of Defense Information Network. Martin and Christey were responsible for analyzing the data made publicly available since 2001 in the vulnerability database.

Martin along with Steve Christey wrote the original vulnerability type distributions document in May of 2007 which provided the basis for categorizing software weakness types in this study (Christey and Martin 2007, 1). Symantec Corporation has become a recognized leader for information security and has published an annual or semi-annual internet security threat report consistently for the past 13 years. The operational context for the U.S. Army when it comes to cyber-attacks and electronic warfare has been provided by ARCIC with the definition of Army Warfighting Challenge #7 (ARCIC 2016). Adrian Graham's book, *Communications, Radar, and Electronic Warfare,* is an excellent source on theory and illustrations for both managers and operators (Graham 2011, 23). The researchers and organizations listed above were particularly important in the completion of this current study.

Statement of the Problem

The problem that the researcher addressed in this study has been defined in the Army Warfighting Challenge #7 (Conduct Space and Cyber Electromagnetic Operations and Maintain Communications) which states, "How to assure uninterrupted access to critical communications and information links (satellite communications [SATCOM], positioning, navigation, and timing [PNT], and intelligence, surveillance, and reconnaissance [ISR]) across a multi-domain architecture when operating in a contested, congested, and competitive operating environment" (ARCIC 2016). The research project was conducted for several reasons. First, the researcher sought to provide a literature review of current threats to communications and network infrastructure which have the potential to disrupt, deny, or degrade the Department of Defense Information Network. Second, the researcher sought to examine some of the current best practices that organizations use for information security like the ones that will be outlined in greater detail as referenced from Symantec Corporation. Third, the researcher sought to conduct a quantitative study of the Common Vulnerabilities and Exposures (CVE) List in order to see if there were trends that could guide decisions for information security professionals. This research study provides value to the U.S. Army Signal Corps because it has examined the current cyber-attacks, and the researcher has made recommendations for future research in cyber-security. This research project benefits scholars and practitioners because it has provided analysis at this current point in time of the trends seen in the CVE List. The data collected from analyzing the CVE List can be used to identify the current trends from specific threat definitions (House 2014, 7).

Scholars and practitioners may be interested in this article because it sought to highlight the threats which the U.S. Army could face against its communications networks while operating in a contested environment. These threats have seemed to come in two basic forms of disruption to networks; the first form of electronic warfare that the researcher categorized are threats that exist in the physical world within the range of the electromagnetic spectrum that are used to disrupt or deny communications capabilities, and the second form of electronic warfare that the researcher described was classified as logical threats which only exist on the network.

The research in this study benefits scholars and practitioners in several more ways. The researcher examined the methods that leading industry security firms have been providing to U.S. Corporations in order to secure their networks against both electromagnetic disruption and logical disruption. The review of the literature has provided a summary of some major security breaches which have occurred in the past ten years. Some of the best practices from the civilian security methods can be applied to military networks in order to maintain communications. Careful analysis of the MITRE Corporation Common Vulnerabilities and Exposures (CVE) List has provided trend information for security strategy decision making purposes.

Purpose of the Study

Army Warfighting Challenge #7 (Conduct Space and Cyber Electromagnetic Operations and Maintain Communications) requires further study to learn, "How to assure uninterrupted access to critical communications and information links (satellite communications [SATCOM], positioning, navigation, and timing [PNT], and intelligence, surveillance, and reconnaissance [ISR]) across a multi-domain architecture when operating in a contested, congested, and competitive operating environment." (ARCIC 2016). The purpose of this study is to understand the current cyber threats and to provide a brief historical background of the cyber-attacks that have occurred in recent global conflicts and in domestic attacks, in order to relate those threats to the potential to cause harm to the Department of Defense Information Network (DODIN). This research is relevant and timely because there has been a renewed focus on the importance of conducting space and cyber electromagnetic operations within the U.S. Army. This research project also explores potential security solutions from leading industry, in order to provide a better understanding of the capabilities required to protect the Department of Defense Information Network in the future from cyber-attacks, common vulnerabilities, and exposures.

Rationale

Research of previous threats will provide a historical basis for the importance of a robust cyberspace and electronic warfare defensive operations strategy. Reviewing current industry standards and best practices for network security will provide an informative summary for Department of Defense leaders to reference and consider for implementation on current networks. Current threats discovered by a quantitative comparison to the types of viruses and malware recorded in the Common Vulnerabilities and Exposures (CVE) List will allow a current view or threat assessment for the types of logical threats detected by the collaborative efforts of cyber security professionals.

Research Questions

Research Question 1

How can the U.S. Army Signal Corps provide security for the Department of Defense Information Network (DODIN) by improving our security posture to withstand the threats form Electronic Warfare methods? As stated earlier, electronic warfare methods can include both physical threats to the network in the form of electromagnetic interference/disruption which can also be called electronic attack, or logical threats such as cyber-attack that occur by unauthorized access to the network. In an attempt to better understand the threat to the DODIN network the subordinate research questions will separate the problem into threats/attacks and defensive measures against these threats.

Research Question 1a

Subordinate research questions include: what major electronic warfare incidents or EW communication disruptions have occurred in the past five years? In military terms these electronic warfare communication disruptions can be classified as offensive attack measures against an adversary. These threats by nature are an act of aggression and potentially an act of war especially when used in conjunction with lethal force.

Research Question 1b

What best practices and methods for improved security can be learned and applied from the practices of private organizations to improve our own Department of Defense Information Network security posture? In military terms these best practices and methods for improved security can be understood or classified as countermeasures to an electronic warfare or cyber-attack.

Research Question 1c

What current threats have been recorded in the Common Vulnerabilities and Exposures (CVE) List and how does this current view or threat assessment for the types of logical threats impact the security decisions for military and Department of Defense cyber security professionals?

Significance of the Study

It is the hope of the researcher, that the significance of this study has been to provide greater depth and understanding of the possible threats against the Department of Defense Information Network based upon the facts discovered in the review of the literature. Other potentially significant results of this study are in the recommendations for future research which will be discussed at greater length later in this report. The analysis of the Common Vulnerabilities and Exposures (CVE) List should prove to be beneficial to scholar-practitioners. The research providing a summary of past threats and a summary of industry best practices for security could also help to inform future Department of Defense cyber security decisions.

Operational Definitions of Key Terms

The following operational definitions will be used for the remainder of this study:

Barrage Jamming: "In barrage jamming a range of frequencies is jammed at the same time. Its main advantage is that it is able to jam multiple frequencies at once with enough power to decrease the [signal-to-noise ratio] SNR of the enemy receivers. However as the range of the jammed frequencies grows bigger the output" (Mpitziopoulos et al. 2009, 44).

Deceptive Jamming: "Deceptive jamming can be applied in a single frequency or in a set of frequencies and is used when the adversary wishes not to reveal her existence. By flooding the [wireless sensor network] WSN with fake data she can deceive the network's defensive mechanisms (if any) and complete her task without leaving any traces. Deceptive jamming is a very dangerous type of attack as it cannot be easily detected and has the potential to flood the PE with useless or fake data that will mislead the WSN's operator and occupy the available bandwidth used by legitimate nodes" (Mpitziopoulos et al. 2009, 44-45).

GSM: "Global System for Mobile Communications" (Graham 2011, xvii).

Spoofing: "Spoofing is a method of using a radio or radar system to mimic the parameters of another system. Using this method, a warship can pretend to be a non-combatant or other vessel. The aim is to fool enemy forces into misidentifying the warship and ignoring it, until it is too late. This is a modern day version of a traditional method of ruse de guerre in which warships used to fly false colours to fool other warships" (Graham 2011, 325).

Spot Jamming: "The most popular jamming method is the spot jamming wherein the attacker directs all its transmitting power on a single frequency that the target uses with the same modulation and enough power to override the original signal. Spot jamming is usually very powerful, but since it jams a single frequency each time it may be easily avoided by changing to another frequency wave" (Mpitziopoulos et al. 2009, 44).

Sweep Jamming: "In sweep jamming a jammer's full power shifts rapidly from one frequency to another. While this method of jamming has the advantage of being able to jam multiple frequencies in quick succession, it does not affect them all at the same time, and thus limits the effectiveness of this type of jamming. However, in a [wireless sensor network] WSN environment, it is likely to cause considerable packet loss and retransmissions and, thereby, consume valuable energy resources" (Mpitziopoulos et al. 2009, 44).

Limitations and Delimitations

Limitations are defined by Creswell as a means to establish the boundaries of a study. The author writes, "Provide limitations to identify potential weaknesses of the study" (Creswell 2003, 167). One potential weakness in this study was that all of the content for this research project has been limited to unclassified information, which is to say that all of the information collected is available for public use. Another limitation for this study was the fact that all data collected would include only data from the publicly available CVE database; this was done in order to simplify the nature of the study by removing all human subjects from the research. Delimitations are also defined by Creswell, “Use delimitations to narrow the scope of a study . . . the scope may focus on specific variables or a central phenomenon, delimited to specific participants or sites, or narrowed to one type of research design (e.g., ethnography or experimental research)” (Creswell 2003, 167). Some delimitations used to narrow the scope of this study included limiting the study to a quantitative research design.

Nature of the Study

The nature of this study was a quantitative research study. The researcher used the same 41 variables or “flaw types” defined by Christey and Martin in their 2007 research study. These flaw types included defined vulnerabilities like cross-site scripting and spoofing. The full list of 41 variables in described in greater detail in table 7. The study included quantitative descriptive analysis which was used to determine common threats or vulnerabilities that were defined in the Common Vulnerabilities and Exposures (CVE) List. The flaw types defined in the CVE List were analyzed in order to determine the frequencies of each flaw type total and the top five flaw type were analyzed to show the frequencies that they occurred each year. Highlighting the common threats by both vulnerability type and by year can assist leaders with planning strategies to protect against potential cyber-attacks and electronic warfare threats in the future. The theoretical/conceptual framework for the study is given in figure 1.

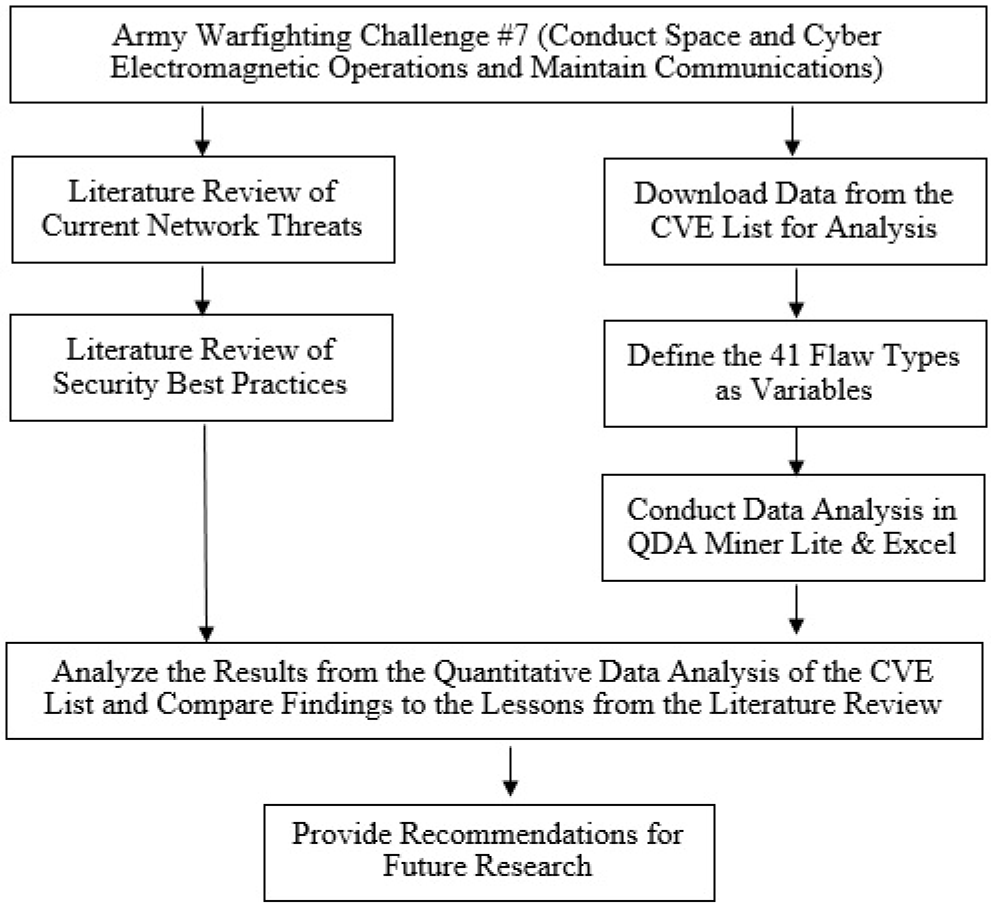


Figure 1. Theoretical/Conceptual Framework

Source: Created by author.

Organization of the Remainder of the Study

The remainder of this study provides a background review of the literature surrounding current cyber-attacks that have taken place within the last decade. Radio jamming and some of the principles of electronic warfare are reviewed briefly. Also, the researcher conducted an inquiry of the methods used by network security professionals to defend against specified threats to their networks. Next, the review of the research done for the CVE List is discussed. A summary of the creation and use of the Common Vulnerabilities and Exposures (CVE) list provides the background for chapter 3 and chapter 4. Chapter 3 provides details on the research methods used to study the data from the Common Vulnerabilities and Exposure (CVE) List. Chapter 4 provides the results of the data analysis. Chapter 5 describes the results and gives suggestions for future research.

CHAPTER 2

LITERATURE REVIEW

Summary of Existing Literature

Threats to the command and control (C2) systems used by the U.S Army, sister services, and allies are susceptible to numerous forms of cyber-attack and electronic warfare threats. One form of cyber-attack can be in the form of logical cyber threats such as hacking. Actions against physical cyber threats like electromagnetic interference/disruption, or in a combination of both effects. Cyber-attacks can be used for different effects such as collection, targeting, and attack on C2 capabilities. These threats are rapidly changing and efforts have been made to collectively categorize computer system vulnerabilities and exposures through efforts such as the creation of the Common Vulnerabilities and Exposures (CVE) List. Future capabilities based assessments will require the consideration of cyber protection and cyber-attack capabilities in order to retain the tactical advantage on the battlefield.

Mixed Cyber Threats: Logical and Physical Effects

Russia has proven that they have developed significant electronic warfare systems with a range of mixed capabilities. The first incident where Russia flexed their electronic warfare capabilities was during their five day conflict with Georgia in August, 2008. This five day war was better planned and organized than the previous conflicts in 1994-1996; the differences being that in 2008 the Russians massed 20,000 troops in South Ossetia in a rapid deployment where they were able to take advantage of cyber warfare and diplomatic offensive techniques. Although Russia's performance was improved compared to their previous Chechen conflict there was still evidence that the use of precision weapons and electronic warfare were not capable of competing with greater global powers (Pallin and Westerlund 2009, 401).

In 2015 reports from the *BBC Monitoring Former Soviet Union* (November, 2015) describe the anti-access (A2) and area-denial (AD) electronic warfare systems used for countering foreign troops within that territory. One system described is the "Rychag-AV helicopter complex, which is capable of "blinding" the adversary's radars at a distance of several hundred kilometres" (Rossiyskaya Gazeta 2015). Another report cited a system called the "Khibiny that raised a furor a year ago when, according to SMI [mass media] information, it shut down radars of the US destroyer Donald Cook in the Black Sea, after which the crew submitted requests to be relieved from the ship" (Segodnya 2015). These reports are based upon information from Russian Media Sources which are state sponsored and should be further scrutinized for reliability. Anti-access and area-denial has been typically a role for ballistic missiles and anti-aircraft artillery, however, "It should be assumed that cyber-attacks will be a part of an opponent's A2/Ad operational approach" (Gordon and Matsumura 2013, 18).

Most recently Russia was able to conduct effective electronic warfare during their attacks in the Ukraine. The report on NPR morning edition explained the spear phishing attack as follows:

> It's masterful—so far as manipulation goes—because of the "lure documents" that attackers use as bait. Lead researcher Jason Lewis gives an example of a Microsoft Word file, dated Jan. 15, 2015. Written in Ukrainian, it's an overview of the situation at the Russia-Ukraine border—apparently authored by Ukraine's State Border Guard Service. The words "not for distribution" are written on it. "That document appears to be something that was on a Ukrainian military computer," Lewis says. Hackers stole the document, then sent it to another

> Ukrainian security agency—with the malware hidden inside. "So the idea being that someone would see: 'Oh, this is news for today. Let me go and take a look and open it.'" The malware would then infect their computer, so that the hackers could extract more classified intelligence: on the numbers of Ukrainian troops in reconnaissance battalions, the equipment they use and the rebel leaders they want. This so-called spear-phishing attack is the same kind that got Sony Pictures. (Shahani 2015)

Russia in the Ukraine has successfully used a cyber spear-phishing attack to deliver effects against the Ukrainian Army. Another article explained that the Ukraine has had to deal with fighting Russia in a severely communications degraded environment; references to electronic warfare, jamming, and collecting are all potential threats (Gould 2015, 1). The implementation of electronic warfare capabilities continue to increase and evolve with time causing a greater threat to command and control systems used by NATO forces.

The anti-access and area denial capabilities have increased significantly in recent history from caltrops to cruise missiles. One recent RAND study pointed out, "Hezbollah in southern Lebanon in 2006 is the most notable recent example of this kind of opponent. In Hezbollah's case, there was considerable support from both Iran and Syria, including the provision of long-range rockets and anti-ship cruise missiles" (Gordon and Matsumura 2013, 6). When non-state actors have access to anti-access and area denial weapons of this level of sophistication it poses an incredible threat to all coalition forces operating within that type of environment. To overcome this type of threat becomes even more of a challenge when simple jamming of a GPS signal is used to disrupt operations (Gordon and Matsumura 2013, 5).

Physical Cyber Threats: Kinetic Effects

Physical cyber threats or kinetic effects are any means of disrupting communications links. These threats exist in the physical world in both conventional kinetic threats and in the form of frequencies used for interference along the range of the electromagnetic spectrum. Conventional weapons can be used to physically destroy communications infrastructure. Interference using directed energy is another way to disrupt communications. First of all, laser jamming is one newly developing form of attack which threatens the physical communications infrastructure and the use of satellite communications over commercially accessible satellites. One report in the *Air and Space Power* journal explained that, "Many adversaries can launch missiles, operate lasers, create jamming, or wage cyber-attacks that can make the cost of doing business with the US government too high with relative ease" (Lungerman 2014, 104). In situations like this satellite access requests over privately owned infrastructure could be denied in the future. This would potentially restrain communications capabilities to the limited amount of bandwidth available over government exclusive satellite resources.

Second, another example of newly developing kinetic weapons that can destroy communications infrastructure is the anti-satellite (ASAT) weapon. China has been reportedly developing their antisatellite weapons capabilities. On January 11, 2007, China successfully tested their hit-to kill anti-satellite (ASAT) weapon by destroying the obsolete Feng Yun-1C weather satellite which most likely required an onboard optical tracker and a closing speed of just more than 8 kilometers per second (Forden 2007, 19). India has increased their development of an ASAT weapon for "dissuasive deterrence posture" (Pandit 2012) with the development of the Agni V missile tested in April 2012.

This was most likely a direct result of China's successful test of the ASAT weapon in 2007 (Pandit 2012). The development of improved anti-satellite (ASAT) weapons continues to change the nature of threats to communications infrastructure which leads to the need for greater protection measures against these advanced threats.

Third, one of the oldest and most commonly used threats to communication networks is the jamming of radio signals in all ranges of the electromagnetic spectrum. One group of researchers provided a quick history of the practice of jamming in the military and the types of jamming conducted (Mpitziopoulos et al. 2009, 44). The researchers explained that jamming radio signals was first discovered around the time of the First World War, and it was used by the Russians and Germans during World War II. They also wrote that historical examples of deceptive jamming from World War II took place when ground radio operators would give false instructions to enemy pilots in their own language.

The types of jamming most commonly conducted were defined by the researchers in four categories; Spot jamming which jams a single frequency with high power, sweep jamming which rapidly shifts full power between frequencies, barrage jamming simultaneously jams a range of frequencies, and deceptive jamming which introduces fake data to a single frequency or multiple frequencies. Numerous methods have been developed to overcome these threats from jamming; these methods include low transmit power to avoid detection, high transmit power to overcome noise interference, changing frequencies to a new channel where jamming is not present, frequency-hopping spread spectrum (FHSS) which rapidly shifts among different frequencies, direct sequence spread spectrum (DSSS) which uses a pseudo-noise digital signal to mask the transmission signal, ultra-wide band (UWB) technology which modulates the signal into very short pulses across a large spectrum of frequency, and antenna polarization which uses line-of-sight antennas with specific physical orientation to shrink the propagation of the radio wave (Mpitziopoulos et al. 2009, 44). The kinetic threats such as lasers, missiles, radio jamming, and ASAT weapons are just a small portion of the effects of electronic warfare that military planners should be concerned with.

Detection of radio signals and intercept networks are two other concerns for communications planning. Enemy forces can detect signals and analyze the frequency and power of the signal in order to gain information about adversary forces. Once the specific frequency is discovered and the power level measured, then the distance from the transmission can be estimated based on knowledge of that type of radio. Graham explains in his book about electronic warfare, “It highlights one fundamental precept of CEW and EW; databases of known system parameters are essential” (Graham 2011, 280). Keeping a database of radio transmission frequency ranges, normal power operational output, and other parameters is therefore critical in understanding the signals intelligence gathered within an area of operations. The capabilities of detection systems are specially designed to cover wide frequency ranges, rapidly scan for signals, provide signals analysis, detect multiple signals simultaneously, and are typically programmable to search for pre-selected channels or signal types (Graham 2011, 283). The interception of radio signals is considerably more complex. For signals to be analyzed they must be “able to identify a particular modulation scheme and then demodulate it in order to receive the baseband transmission” (Graham 2011, 284). If the is signal has been encrypted then it will require the right spreading code to reconstruct the signal. Graham explained, “In such cases, recodings of the signal must be sent to a central facility such as the NSA in the US or GCHQ in the UK" (Graham 2011, 285).

The importance of antenna placement for military planners becomes increasingly important when you begin to have communication systems, detection systems, radar systems, and intercept system all working within close proximity of one another. Terrain analysis for antenna placement and careful use of directional antennas can improve system operations, assist with signals intelligence collection efforts, and reduce noise interference from friendly and coalition systems. Graham also explained the complexity of direction finding systems which uses various techniques to locate radio signal locations; Doppler direction fining systems, Watson-Watt direction finding systems, and interferometer direction finding systems all use slightly different antenna placement and signals analysis methods to locate the enemy signal transmission. It is equally important that direction finding information can be provided in real time so that it is useful to military commanders which means that communications with the direction finding systems must be uninterrupted (Graham 2011, 299-314).

GPS jamming is becoming increasingly important as more systems are developed which rely on directional information. Graham explains, "GPS receivers also work on relatively small signals, making them vulnerable to noise, interference and intentional jamming. Trials have shown that GPS is vulnerable to white noise, CW, AM, FM and swept jamming" (Graham 2011, 328). The strength of the noise signal simply needs to overpower the GPS signal to disrupt normal operation of the system. Other methods to transmit deceptive or false GPS signals can be used to cause GPS receivers to follow a different course (Graham 2011, 328).

Logical Cyber Threats: Computer Hacking

Computer hacking is probably the most rapidly changing threat that comes to mind when considering cyber-attacks and the threats against computer assets and infrastructure. Electronic Warfare threats have come in numerous forms and are evolving as time passes so that the threats are becoming more complex and sophisticated. Hacking can be considered a logical threat, as opposed to a conventional kinetic threat like missiles, or a threat that exists within the range of the electromagnetic spectrum like radio interference and jamming.

One of the earliest notable international hacking incidents was the incident conducted by "hacktivists" against Estonia in 2007 (Schmitt 2013, 16). In Estonia the government had made the decision to move a memorial of the Soviet liberation of Estonia from the Nazis to a "less prominent and visible location in Tallinn" (Herzog 2011, 49). The Bronze Soldier was a symbol of Soviet Oppression to the Estonian majority, but to the 26 percent of the population whom had moved to Estonia from Russia, "its relocation represented further marginalization of their ethnic identity" (Herzog 2011, 51). Herzog further explained that riots erupted throughout the country and extensive denial of service attacks ensued crippling the computer systems in Estonia. Following these events, "in 2009 the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), and international military organisation based in Tallinn, Estonia," invited experts to draft the first manual governing the laws of cyber warfare which is titled the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt 2013, 16).

The Tallinn Manual includes 95 rules organized into seven chapters on topics which include the use of force, conduct of attacks, and neutrality to name a few. Section

Two of the manual covers State Responsibility and specifically Rule 7 appears to be a legal loophole for state sponsored hacking; the manual reads, “The mere fact that a cyber operation has been launched or otherwise originates from government cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation” (Schmitt 2013, 39). The manual also notes that “spoofing” in order to disguise the location of origin of an attack is relevant to this rule and “was demonstrated by the incidents involving Estonia (2007) and Georgia (2008) (Schmitt 2013, 40). As the manual implies a similar incident occurred in Georgia in 2008 where denial of service attacks were successfully used.

Distributed denial of service (DDoS) attacks are one form of cyber-attack that has been used in many ways to disrupt computer operations. In the country of Georgia, denial of service attacks occurred back to back on 19 July 2008 and then again on 8 August 2008. These attacks coincided with Russian troop movements into South Ossetia which appeared to be in response to Georgian military operations that had begun on 7 August 2008. By the time the Russian troops were moving into the area most of the Georgian government web sites were down (Korns 2009, 60). Disrupting the Georgian governmental communications and computer capabilities prior to movement into the area was an obvious shaping operation for the Russian military which had the desired effect. The Georgian government was not able to communicate, but even more importantly, the author explained, “Without first obtaining US government approval, Georgia relocated critical official Internet assets to the United States, Estonia, and Poland . . . [which] provides an intriguing opportunity to examine a more subtle and perhaps overlooked aspect of cyber conflict—the concept of cyber neutrality” (Korns 2009, 60). Because the government of Georgia was able to use private IT companies from within the United States for “cyber refuge” this could have some impact on U.S. cyber neutrality even though the actions within private organizations and without U.S. government permission (Korns 2009, 61). It is important to note that Russia has not claimed responsibility for the actions against Georgia in 2008 during the South Ossetia War (Bussing 2013, 5). Policy makers will need to consider the possibility of responding to actions conducted within private organizations in future cyber conflicts. Cyberspace defensive operations will need to be developed to react and defeat these Distributed Denial of Service attacks when they occur.

An extremely large scale hacking attack occurred on August 15, 2012, when Saudi Aramco, one of the world’s largest oil companies, administrative computer network was hacked and computer hard drives were erased. The attack occurred when hackers gained access after a scam e-mail was opened, and a bad link was clicked which allowed access; “In a matter of hours, 35,000 computers were partially wiped or totally destroyed” (Pagilery 2015, 1). The “Shamoon” virus that infected the oil company was examined by researchers at Symantec, a Silicon Valley security company, where they found the word “Shamoon” embedded in its code; the virus, “was designed to do two things: replace the data on hard drives with an image of a burning American flag and report the address of infected computers” (Perloth 2012a, 1).

Other major incidents of hacking have occurred in the recent past which have caused physical damage to infrastructure. Perloth explained one other incident where, “The New York Times reported in June [2012] that the United States, together with Israel, was responsible for Stuxnet, the computer virus used to destroy centrifuges in an

Iranian nuclear facility in 2010" (Perloth 2012a, 2). The details of this incident are described more in depth by the author Dev in the *Texas International Law Journal* quoted here:

> In June 2010, the world discovered that the Stuxnet virus, a wireless malware virus that was able to transcend public Internet, attacked programmed computers at Iran's largest nuclear facilities and caused large-scale breakdowns in Iran's nuclear operations. The malware worm, described as a "sophisticated computer program designed to penetrate and establish control over remote systems in a quasi-autonomous fashion," targeted computer programming systems at Iran's nuclear facilities—ultimately entirely reprogramming many of the systems struck. The bug invaded the computes, lurked for days or weeks, and ultimately sent instructions to speed the nuclear centrifuges up or slow them down so that started spinning at supersonic speeds and ultimately self-destructed. One German expert that studied Stuxnet described it as a "military-grade cyber missile that was used to launch an 'all-out cyber strike against the Iranian nuclear program.'" With the click of a button, a conglomerate of State and non-State actors, allegedly including the United States and Israel, managed to bring major breakdown to Iran's Natanz nuclear fuel enrichment plant with some estimates indicating that the Stuxnet worm led to a 23% decline in the number of operating centrifuges between mid-2009 and mid-2010. (Dev 2015, 398)

The severity of damage done to the physical equipment at this facility increased the perceived strength of cyber-attacks and introduced cyber-attacks as a means for kinetic effects capable of achieving strategic goals.

In another hacking incident, which took place in September 2012, six US banks were the victim of denial of service attacks which disrupted their online banking services (Perloth 2012b, 1). This attack, which was reported to have come from Iran, was ultimately stopped with defensive measures through coordination with authorities in over 100 different countries, but this defensive posture is seen by some to be too weak to deter future cyber-attacks against U.S. institutions (Dev 2015, 394). The back and forth cyber-attacks are not limited to Iran vs. the United States, but have also included attacks from North Korea aimed at the U.S.

North Korea is suspected of conducting state sponsored hacking of Sony Pictures following the creation the movie "The Interview" which involved a comedic plot to kill the North Korean leader Kim Jong-Un (Pagilery 2014, 1). Haggard and Lindsay reported on this incident of a state sponsored cyber-attack explaining two reasons which make this incident significant:

> The Sony hack is one of only a few instances in history of an attempt by a nation state to use cyberspace for explicitly coercive purposes. The Sony hack was also notable because the US government vigorously and publicly rallied to the defense of a private firm targeted for such coercion. (Haggard and Lindsay 2015, 3)

This incident proved to gain public support from the federal government defending Sony. The FBI also issued public statements accusing North Korea of the attack which took place in November 2014, and the State Department spoke publicly about a "range of options in response . . . [noting that] some will be seen, and some may not be seen" (Daugirdas and Mortenson 2015, 420). Later reports showed that internet outages were experienced in North Korea due to denial of service attacks and officials simply stated "accidents can happen" (Daugirdas and Mortenson 2015, 420). Iran and North Korea have also been joined by advanced persistent threats (APTs) that have been traced back to China.

China has been accused of committing the theft of information against the Office of Personnel Management (OPM) which included scores of information on U.S. federal employees. One of the most disturbing pieces of information stolen as a result of this hack was the security clearance background check data (also called SF-86 data) for 2.1 million current federal civilian employees and 2 million retired federal civilian employees (Nakashima 2015, 1). Previous hacks connected to the Chinese government were made against a contractor that conducted background investigations for the OPM and the Department of Homeland Security (Nakashima 2015, 1). Nakashima (2015) also explained that potential uses of information about federal employees could be directed at discovering the identity of Central Intelligence Agency (CIA) agents or counter espionage, or China could use the information to blackmail individuals with ties to federal employees with valuable information. Ongoing threats from China are reported in other articles where, “According to a report from Mandiant, an independent computer security company, Unit 61398 has stolen information from 150 companies for a period of seven years, and has accumulated more than a hundred terabytes of data” (Bussing 2013, 12). This kind of espionage against U.S. Business and theft of government information is not currently defined within the laws of armed conflict, therefore policy makers must use guidance contained within executive order 12958 which categorizes the significance of stolen information into five categories displayed in table 1 (Bussing 2013, 12).

Table 1. Executive Order 12958
1. A Type 1 attack causes a nuisance or inconvenience to the defense or economic security of the United States.
2. A Type 2 attack causes damage to the defense or economic security of the U.S.
3. A Type 3 attack causes serious damage to the defense or economic security of the U.S.
4. A Type 4 attack causes exceptionally grave damage to the defense or economic security of the U.S.
5. A Type 5 attack causes critical damage to the defense or economic security of the U.S.

Source: Joseph Bussing, “The Degrees of Force Exercised in the Cyber Battlespace,” *Connections: The Quarterly Journal* 12, no. 4 (2013): 1-13, accessed January 17, 2016, https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/1501475997?accountid=28992.12.

Best Practices for Security

For the past 13 years Symantec Corporation has published an annual or semi-annual internet security threat report. Last year, in April of 2015, the Volume 20 report included a fairly comprehensive summary on what types of threats businesses and individuals can expect. The report from Symantec categorized threats into the following primary groups: Mobile devices and the Internet of Things, Web Threats, Social Media and Scams, Targeted Attacks, Data Breaches and Privacy, and E-Crime and Malware. Each of these groups include more narrowly defined threats such as browser vulnerabilities, e-mail phishing, total breaches, and crypto-ransomware to name just a few (Symantec 2015, 4). The report from April 2014 included tips for protection against these threats for both businesses and individuals. These best practice guidelines for businesses are summarized in table 2.

Table 2. Best Practice Guidelines for Businesses
1. Employ defense-in-depth strategies.
2. Monitor for network incursion attempts, vulnerabilities, and brand abuse.
3. Antivirus on endpoints is not enough.
4. Secure your websites against MITM attacks and malware infection.
5. Protect your private keys.
6. Use encryption to protect sensitive data.
7. Ensure all devices allowed on company networks have adequate security protections.
8. Implement a removable media policy.
9. Be aggressive in your updating and patching.
10. Enforce an effective password policy.
11. Ensure regular backups are available.
12. Restrict email attachments.
13. Ensure that you have infection and incident response procedures in place.
14. Educate users on basic security protocols.

Source: Symantec Corporation, *Internet Security Threat Report*, Volume 19 (Mountain View, CA: Symantec Corporation, 2014), 87-88, accessed January 17, 2016, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

These 14 best practice guidelines for businesses are a good general summary for reviewing an organization's network and information security posture. While these best practice guidelines will assist with the protection from logical or hacking attacks, other measures will need to be employed to protect the physical links of the network.

Protection from physical attack of the network must be achieved by employing the best practices for countering enemy communications electronic warfare. The tactical methods for countering enemy communications electronic warfare (CEW) include the following:

Table 3. Tactical Methods of Countering Enemy CEW
1. Power minimization.
2. Minimizing transmissions.
3. Using antennas as low as possible.
4. Use of directional antennas.
5. Orienting directional antennas away from the enemy (or parallel to the FLOT).
6. Using low probability of intercept systems such as spread spectrum.
7. Using other traffic to mask own transmissions, such as using unused channels in GSM networks for example.
8. Making use of terrain and clutter shielding.
9. Using spoofing.

Source: Adrian Graham, *Communications, Radar and Electronic Warfare* (Hoboken, NJ: John Wiley and Sons, 2011), 325.

Other tactical methods of countering enemy communications electronic warfare listed in ATP 6-02.53 are to, "change network call signs and frequencies often (in accordance with the signal operating instructions); use approved encryption systems, codes, and authentication systems; make electronic protection equipment requirements known; and ensure quick repair of radios with mechanical or electrical faults [which] is one way to reduce radio-distinguishing characteristics" (Department of the Army 2016, 12-3). The Army doctrine also emphasizes that electronic protection is a command responsibility, yet the G-6 and the S-6 will prepare and conduct the electronic protection training program. While organizations must employ these best practices to protect against logical internet security threats and physical electronic warfare threats, trend analysis of the Common Vulnerabilities and Exposures (CVE) List will provide insight to information technology professionals and U.S. Army Signal Corps leaders on the current threats to the network.

Common Vulnerabilities and Exposures (CVE) List

The MITRE Corporation Common Vulnerabilities and Exposures (CVE) List is an open source dictionary of publicly known information security vulnerabilities and exposures (MITRE 2016). The frequently asked questions section from the CVE website gives some background information about the use and purpose of the CVE List. The site explains:

> CVE is sponsored by US-CERT the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. Operating as DHS's Federally Funded Research and Development Center (FFRDC), MITRE has copyrighted the CVE List for the benefit of the community in order to ensure it remains a free and open standard, as well as to legally protect the ongoing use of it and any resulting content by government, vendors, and/or users. (CVE 2016)

The benefits for keeping this list as an open source tool allows anyone to contribute to the known virus definitions. Once definitions are accepted to the list it allows standardization for that virus definition to take place and the person who discovered and defined the virus is given credit for the discovery and sometimes can be reward with monetary incentives. By analyzing the CVE List the researcher can provide a current picture of the known virus definitions. Previous research on this subject was conducted by Robert Martin from the MITRE Corporation where he created what he called, “the use of standard knowledge representation, enumerations, exchange formats and languages, as well as sharing of standard approaches to key compliance and conformance mandates” (Martin 2008, 1). In this paper he defined the Common Vulnerabilities and Exposures (CVE) as the, “Standard identifiers for publicly known vulnerabilities” (Martin 2008, 3). Martin along with Steve Christey wrote the original vulnerability type distributions document in May of 2007 after completing five years of tracking errors that lead to publicly reported vulnerabilities (Christey and Martin 2007, 1). In their research they found that the quantity of vulnerabilities was rising each year and that the types of vulnerabilities were noticeably different (Christey and Martin 2007, 2). While Martin and Christey conducted the initial research for the CVE List, other researchers have expanded on their work since 2007 and 2008.

Trend analysis and methods for ranking attacks and vulnerabilities has been conducted by researchers in 2010 and 2012. First of all, Stephan Neuhaus and Thomas Zimmermann used machine learning to discover trends within the 39,393 unique CVE that had been identified through the end of 2009. The researchers explained that this was the first independent study on the entire body of the CVE database outside of MITRE Corporation and they found that, "well known vulnerabilities like buffer overflows and format strings are declining . . . SQL injection and cross-site scripting have dents in their growth curve of the last few years" (Neuhaus and Zimmermann 2010, 1-6). The researchers analyzed the text of the Common Vulnerabilities and Exposures (CVE) List in order to identify these trends. Second, Wang, Guo, Wang, and Zhou conducted their study to measure and rank attacks based on vulnerability analysis using the "14 types of vulnerabilities that have been mapped to attack patterns of [the Common Attack Pattern Enumeration and Clasification] CAPEC" (Wang et al. 2012, 458). The researchers then provided a brief description of the top ten attacks for Internet Explorer 7 based upon their classifications and many of the threats were various types of buffer overflow (Wang et al. 2012, 485).

Patterns and Gaps in the Literature

The most recent research analyzing the trends or types of common vulnerabilities and exposures was conducted in 2012 by Wang, Guo, Wang and Zhou. Since then thousands more vulnerabilities have been defined and added to the list. Current research on this list would fill the gap in the literature where no additional analysis has been published regarding the current trends in vulnerabilities. This research project provides up to date analysis on the Common Vulnerabilities and Exposures (CVE) List in order to report on the current trends. There also appears to be gaps in the literature describing physical effects of electromagnetic disruption to command and control capabilities. Further details on the cyber and electronic warfare capabilities of other nations is limited at this time and is limited by the nature of this study. Some interviews with network security professionals in future research could give a greater depth of information on the specific threats that security professionals face on a daily bases. Other qualitative studies or reviews of the data from the Common Vulnerabilities and Exposures (CVE) List could show trends for certain types of vulnerabilities that were not defined in the original list of 41 flaw types.

CHAPTER 3

RESEARCH METHODOLOGY

Research Methods

After conducting the literature review the researcher discovered that analysis on the Common Vulnerabilities and Exposures (CVE) List could be studied in order to identify trends in security threats. The study was slightly modified from the original study conducted by Christey and Martin in 2007. Christey and Martin used 41 separate descriptions of common vulnerabilities and exposures. They measured the frequency of each type of flaw and charted the trends over each year. They also measured the top 5 and top 10 diversity percentages per year, which was a percentage of the total number of reported vulnerabilities made up of the top 5 and top 10 most frequently occurring vulnerabilities. The data in the current study was analyzed as closely as possible using the same measures as were used in the previous study in 2007 in order to provide easy means of comparing the results of the two studies.

In this study a quantitative data analysis on the text information contained in the CVE List was conducted. The data was analyzed using several different variables. The total data set was analyzed for the total frequency of flaws defined per year, and individual flaws were analyzed to determine their frequency throughout the history of the CVE List. The methodology chosen reflects the methods originally conducted by Christey and Martin in 2007 with some modifications based on limitations of the current study. The variables selected for the study were categorized by calendar year and by the 41 separate terms for flaws which were first defined by Christey and Martin in 2007 (Christey and Martin 2007, 18-24). Those flaws were the most common flaw definitions.

The CVE List was downloaded from http://cve.mitre.org/data/downloads/index.html on January 25, 2016, in the comma separated values format file titled “Raw (.csv)”. The CVE Version number was listed as 20061101. Once the list was downloaded the researcher viewed the list in Microsoft Xcel in order to remove lines 1, 2, 4-10, which had text notes; line three was used as the variable name and lines 11 through 87,893 became the data set. The final list included entries CVE-1999-001 through CVE-2016-2068; this was a total of 87,883 entries or individual vulnerabilities/exposures.

The qualitative data analysis software tool, QDA Miner Lite, was used to analyze the .csv file containing all of the CVE List entries. All 87,883 entries were imported to QDA Miner Lite. Variables were kept as listed in the CVE List. There were seven variables provided by default in the CVE List by downloading the entire .csv file; those variables were titled “Name, Status, Description, References, Phase, Votes, and Comments”. In the research report from Christey and Martin from 2007, the researchers used 41 distinct flaw terminology types to describe the items in the CVE List. These 41 types or flaw terms were added as codes in QDA Miner in order to get a total count of each type within the complete set of 87,883 cases. Codes were also defined to separate the cases by the year in which they were defined. The CVE List name identifier was modified into a new case in order to capture the information for the year in which each flaw was defined. Grouping the definitions by the year that they were defined allowed for comparison to the results published by Christey and Martin. The retrieval tool in QDA Miner Lite was then used to code all cases to match the description of each of the 41 types. The search unit was set to “Documents” in order to only count each case one time. QDA Miner Lite was limited in the data analysis that it would conduct, therefore

Microsoft Xcel was used in order to count the exact number of the top five flaws occurring during each calendar year. Xcel was useful because the text could be analyzed, color coded, and filtered by on the conditional formatting tools. Using the function to format the data as a table was also helpful in the final analysis of the data. Only the top 5 flaws were analyzed to get the data for frequencies of each flaw during each calendar year.

Population/Sample

The sample included 87,883 individual entries from the Common Vulnerabilities and Exposures (CVE) List. Each CVE identifier is made up of three distinct parts. First there is the "CVE Identifier number (e.g., "CVE-1999- 0067", "CVE-2014-12345", "CVE-2014-7654321")". Second there is the, "Brief description of the security vulnerability or exposure". The third part of the CVE is "Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID)" (CVE 2016). The name of each case, or the CVE identifier, was used to assign a new variable which the researcher titled "year" in order to allow for easy comparison to the results of previous studies. The 87,883 cases were each included in the results that follow in chapter 4.

Setting

All data was taken directly from the CVE.MITRE.org website from free and open source materials. When downloading the CVE the format can be selected from various types, but for the purpose of this research the comma separated values data format was selected for easy translation into Microsoft Excel and QDA Miner Lite for further analysis.

Instruments/Measures

Instrumentation will include the use of qualitative data analysis software, QDA Miner Lite, and Microsoft Excel to analyze the data set downloaded. QDA Miner Lite was chosen as the software analysis tool because of its capabilities for analyzing raw text data like the data which is included in the "description" column of the CVE List .csv file. Measures of the data included quantitative measures on the frequencies of specific types of vulnerabilities per year and the frequencies of those vulnerabilities as related to the total number of cases since the CVE List was made public in 2001. The qualitative measures to discover recurring themes in the type of threats defined within the Common Vulnerabilities and Exposures (CVE) list will have to be included in the recommendations for future research. For the purposes of this study, only the currently defined 41 flaws used by Christey and Martin in 2007 were used for data analysis.

Data Collection

Data collection was conducted using publicly available information from the CVE data set from US-CERT and MITRE Corporation. The CVE List was downloaded from http://cve.mitre.org/data/downloads/index.html on January 25, 2016, in the comma separated values format file titled "Raw (.csv)". The CVE Version number was listed as 20061101. Data collection did not include the participation from any human subjects. All data is available for public use in order to promote the common enumeration and to promote sharing of information related to threats.

Data Analysis

Frequency tables were used to determine the number of vulnerabilities defined each year and charts showing the changes in frequency each year have been displayed in chapter 4. Text mining using QDA Miner Lite could not be conducted on the set of 87,883 entries or individual vulnerabilities/exposures which have been defined during the period of time from 1999 until the data set was downloaded on January 25, 2016, because those features are not activated in the Lite version of the software. Instead the analysis on each individual flaw per year was conducted using Microsoft Xcel with conditional formatting. Conducting the analysis with Xcel proved to be slightly more time consuming and therefore, only the top 5 vulnerabilities were analyzed for the frequency per year.

Validity, Reliability, Credibility, Transferability, Dependability, and Trustworthiness

Most quantitative data testing will not fit the data collected because the data is mostly free text without a uniform structure. This is why the data set was analyzed using a qualitative data analysis tool and then analyzed for the frequency of occurrence. The text descriptions of the security vulnerability or exposures were analyzed for trends. The validity of an instrument is described in terms of “whether one can draw meaningful and useful inferences from scores on the instruments” (Creswell 2003, 179). The frequencies reported from the data collected are meaningful and can be compared to previous research. The reliability of this study can be checked by subsequent researchers because the data set is available to the public for use and the methods used are described in detail.

Ethical Considerations

Ethical considerations do not apply to data collection portion of this research study because human subjects were not directly involved in this research. Creswell described ethical issues in the research problem, the purpose and questions as well. The problem does not appear to marginalize or disempower any particular group, and the purpose or questions are not deceptive in nature again because human participants were not used in the collection of this data (Creswell 2013, 88).

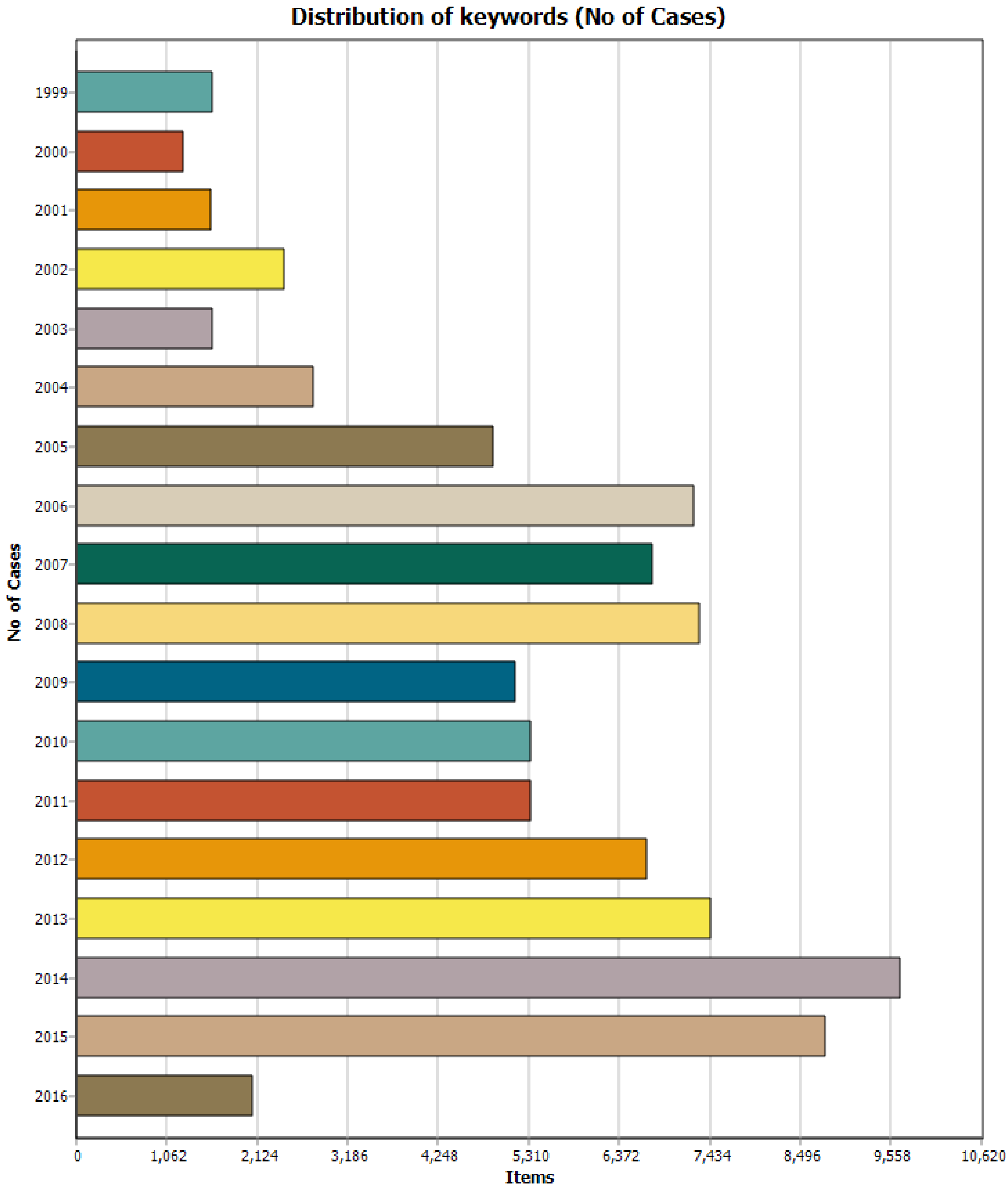
CHAPTER 4

ANALYSIS

The results listed below were derived from data from the CVE List from the total number 87,883 cases on record from 1999 through January 25th, 2016. The analysis conducted shows the number of Common Vulnerabilities and Exposures defined by the 41 flaw types and by number of cases per year which uses the same 41 flaw types as defined by Christey and Martin in 2007. The 41 flaw types defined by Christey and Martin were used as variables for analysis of the data set. The frequency of occurrence for those 41 types resulted in a total of 69,753 cases being counted in the analysis of the total 87,883 cases. That is 79.37 percent of the total number of cases. Comparatively, in 2007 when Christey and Martin first analyzed the CVE List they had approximately 4,000 out of 18,809 cases defined as “other” or “not specified”. This means that 78.73 percent of the total number of cases fit into the definitions of the vulnerabilities and exposures, or flaws, created by Christey and Martin in 2007. The researchers explained that it was more cost efficient to use the most frequently occurring definitions to categorize the vulnerabilities and exposures, rather than trying to define hundreds or thousands more flaws each time the data set was analyzed cases (Christey and Martin 2007, 17).

Table 4 displays graphically the trend in the increasing number of cases since 1999. The number of total defined Common Vulnerabilities and Exposures began at 1,592 per year in 1999 and has grown to a total of 8,787 defined vulnerabilities in 2015. The most definitions in one year occurred in 2014 with 9,659 definitions added to the CVE List. The first six years had an average number of vulnerabilities of 1,870, with the greatest number at that time being 2,778 reported cases in 2004. There was a dramatic increase in the total number of vulnerabilities defined per year beginning in 2005. The total number of cases was more than double the six year average of 1,870, with 4,895 vulnerabilities defined in 2005. This spike was followed by another huge jump to an average of 7,111 vulnerabilities per year from 2006 to 2008. The first six year average from 1999 to 2004 was 1,870 cases per year. The next six year average from 2005 to 2010 was 6,117 cases per year. Even with only one month of data in 2016, the next six year average for 2011 to 2016 was 6,666 new vulnerabilities defined each year. The data for this study only included the vulnerabilities through January 25th, 2016, but as of May 2nd, 2016 there were 4,427 vulnerabilities defined. Substituting the 2,029 cases reported in January for the 4,427 cases reported through May brings the six year average up to 7,059 vulnerabilities defined per year. Therefore, since 2004 until 2016, the six year average has increased by almost 4 times the number of vulnerabilities defined each year.

Table 4. Total CVE Definitions Each Year



Source: Created by author.

Table 5 shows the exact count for the number of newly defined vulnerabilities and exposures each year. This is the same data shown in table 4 as a bar chart. The least number of vulnerabilities and exposures reported in one year occurred in the year 2000 with 1,244 cases. The highest number of cases in one year occurred in 2014 with 9,659 total newly defined vulnerabilities and exposures.

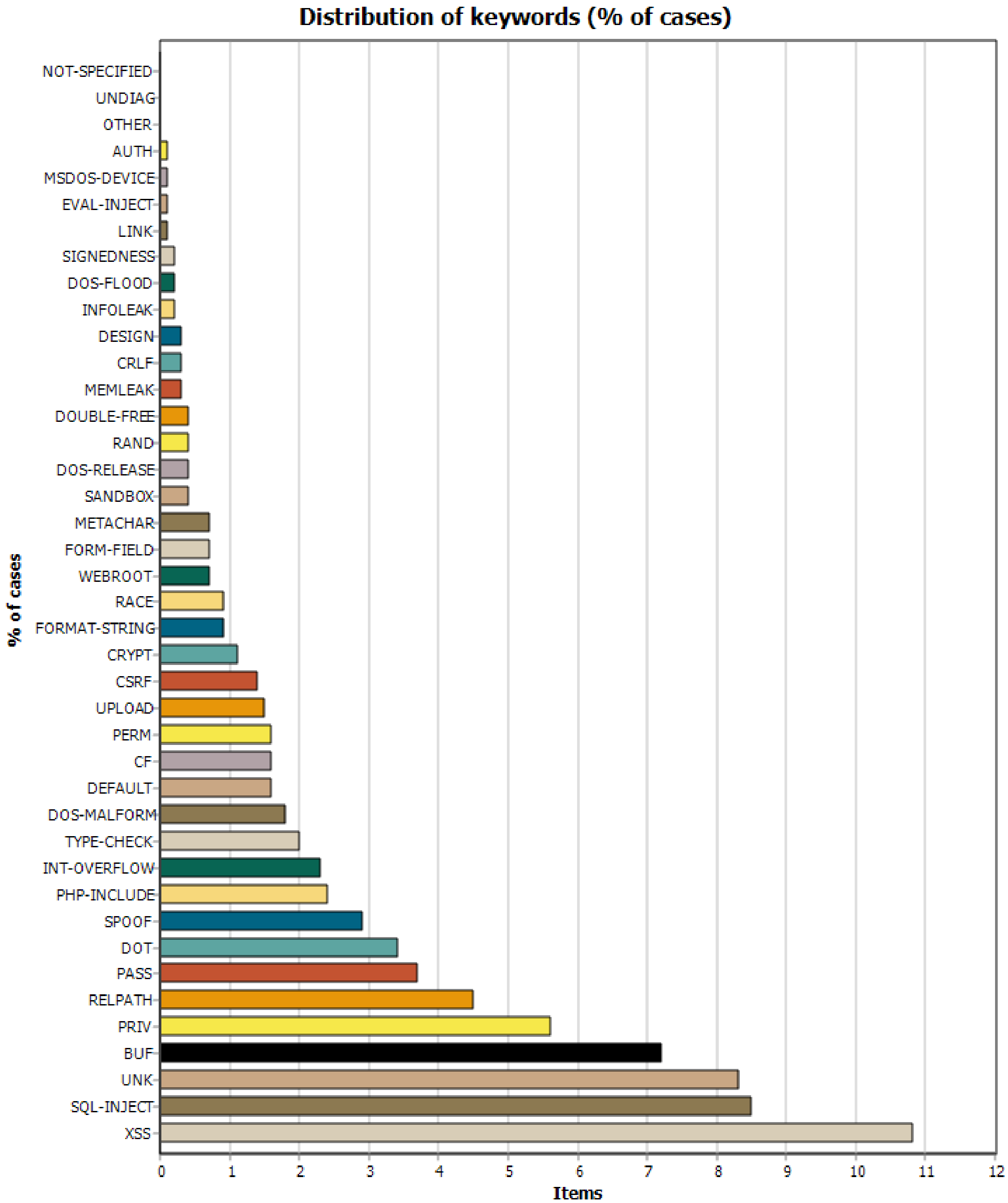
Table 5. Total Number of CVE Definitions Each Year Specified

Year	No of Cases
1999	1592
2000	1244
2001	1574
2002	2434
2003	1598
2004	2777
2005	4893
2006	7253
2007	6758
2008	7316
2009	5149
2010	5324
2011	5330
2012	6700
2013	7446
2014	9659
2015	8785
2016	2068

Source: Created by author.

Table 6 shows the distribution of flaws by category as a total percentage of the 87,883 cases on record from 1999 through January 25th, 2016. As shown in this table the Common Vulnerability and Exposure with highest percentage of overall cases was the XSS variable, which is an abbreviation for cross-site scripting (XSS). Table 6 provides a good visual comparison of each of the pre-defined vulnerability types by showing them in order from the least occurring at the top of the table to the most frequently defined XSS. In comparison to Christey's earlier research, the top 5/10 diversity percentages are figured from table 7 and displayed in table 8.

Table 6. Total Percentage of Individual Flaws



Source: Created by author.

It is helpful to see the data represented in a bar graph and organized from the least to most occurring frequency, but it is also helpful to view the raw numbers in a table. While table 6 shows a comparison of each vulnerability in a bar graph as a percentage of the whole data set from 1999 until January 2016, table 7 shows the exact number of cases for each type of vulnerability listed in a table. Additionally, the descriptions provided by Christey are listed in this table (Christey and Martin 2007, 18-24).

Table 7. Description and Total Number of Each Flaw

ABBREVIATION	FLAW TERMINOLOGY	NUMBER
AUTH	Weak/bad authentication problem	3090
BUF	Buffer overflow	6326
CF	General configuration problem, not perm or default	1428
CRLF	CRLF injection	221
CRYPT	Cryptographic error	948
CSRF	Cross-site request forgery (CSRF)	1252
DEFAULT	Insecure default configuration, e.g., passwords or permissions	1387
DESIGN	Design problem, generally in protocols or programming languages	268
DOS-FLOOD	DoS caused by flooding with a large number of legitimately formatted requests	191
DOS-MALFORM	DoS caused by malformed input	1569
DOS-RELEASE	Dos because system does not properly release resources	327
DOT	Directory traversal	2974
DOUBLE-FREE	Double-free vulnerability	333
EVAL-INJECT	Eval injection	118
FORM-FIELD	CGI program inherently trusts form field that should not be modified	617
FORMAT-STRING	Format string vulnerability	779
INFOLEAK	Information leak by a product	133
INT-OVERFLOW	A numeric value can be incremented to the point where it overflows and begins at the minimum value, with security implications	1995
LINK	Symbolic link following	45

MEMLEAK	Memory leak (doesn't free memory when it should)	258
METACHAR	Unescaped shell metacharacters or other unquoted special char's; currently includes SQL injection but not XSS	611
MSDOS-DEVICE	Problem due to file names with MS-DOS device names	71
NOT-SPECIFIED	The CVE analyst has not assigned a flaw type to the issue; typically similar to other	11
OTHER	Other vulnerability; issue could not be described with an available type at the time of analysis	0
PASS	Default or hard-coded password	3285
PERM	Assigns bad permissions, improperly calculates permissions, or improperly checks permissions	1449
PHP-INCLUDE	PHP remote file inclusion	2128
PRIV	Bad privilege assignment, or privileged process/action is unprotected/unauthenticated	4899
RACE	General race condition (not symbolic link following (link)!)	782
RAND	Generation of insufficiently random numbers, typically by using easily guessable sources of random data	312
RELPATH	Untrusted search path vulnerability	3915
SANDBOX	Java/etc. Sandbox escape - not by dot-dot!	206
SIGNEDNESS	Signedness error	175
SPOOF	Product is vulnerable to spoofing attacks	2519
SQL-INJECT	SQL injection vulnerability	7511
TYPE-CHECK	Product incorrectly identifies the type of an input parameter or file	1733
UNDIAG	Undiagnosed vulnerability	1
UNK	Unknown vulnerability; report is too vague to determine type of issue	7297
UPLOAD	Product does not restrict the extensions for files that can be uploaded to the web server	1279
WEBROOT	Storage of sensitive data under web document root with insufficient access control	622
XSS	Cross-site scripting (aka XSS)	9509

Source: Steve Christey and Robert A. Martin, “Vulnerability Type Distributions in CVE.” 2007, accessed January 17, 2016, https://cve.mitre.org/cve/identifiers/index.html, 18-24.

Table 8 provides a percentage of the total cases that were the top five and top ten vulnerabilities from 1999 until January 25th, 2016. This is a percentage of the total 87,883 defined vulnerabilities and exposures in the CVE List through that date. When Christey and Martin conducted the initial study in 2007, they analyzed a total of 18,809 cases. The total top five vulnerabilities from the previous research by Christey and Martin represented 46.1 percent of the total 18,809 cases; the top ten represented 57.3 percent of the total 18,809 cases. The results from the current study are displayed in table 8. The current study showed that the top five cases declined to 40.44 percent while the top ten represented 58.4 percent of the total vulnerabilities and exposures defined. This means that the top ten threats are even more of a threat now and are more commonly the exploited weakness of choice for hackers.

Table 8. Top 5 and Top 10

Top n	TOTAL Percent through 2016	Total Cases through 2016	TOTAL Percent through 2007
5	40.44%	35,542	46.10%
10	58.40%	51,325	57.30%

Source: Created by author.

Table 9. Top 10 Comparison from 2007 to 2016

Rank	Flaw 2007	Total through 2007	Flaw 2016	TOTAL through 2016
Total		18809		87883
[1]	XSS	13.80%	XSS	10.82%
		2595		9509
[2]	buf	12.60%	sql-inject	8.55%
		2361		7511
[3]	sql-inject	9.30%	unk	8.30%
		1754		7297
[4]	php-include	5.70%	buf	7.20%
		1065		6326
[5]	dot	4.70%	priv	5.57%
		888		4899
[6]	infoleak	3.40%	relpath	4.45%
		646		3915
[7]	dos-malform	2.80%	pass	3.74%
		521		3285
[8]	link	1.80%	auth	3.52%
		341		3090
[9]	format-string	1.70%	dot	3.38%
		317		2974
[10]	crypt	1.50%	spoof	2.87%
		278		2519

Source: Created by author.

Another useful comparison is to look at which specific vulnerabilities and exposure made the top ten list in 2007 compared to the top ten list from this current study. Table 9 provides the side by side comparison of the top ten vulnerabilities and exposures as observed by Christey and Martin in 2007 and by the current research from this study. The current top ten most common threats make up an increasing percentage of the total number of vulnerabilities and exposures defined each year, which means that greater emphasis should be placed on preventing those types of vulnerabilities and exposures from occurring. Also, it is significant that the types of vulnerabilities and exposures which made the top ten list in this study are different from those which were in the top ten list in 2007. Still the most common threat is cross-site scripting or XSS. The other vulnerabilities which are still in the top ten include SQL injection vulnerability, buffer overflow, and dot or directory traversal. The new or up and coming threats in the top ten list from this current study include unknown vulnerabilities, bad privilege assignment, relpath or untrusted search path vulnerability, default or hard-coded password, weak/bad authentication problem, and spoofing attacks.

Further analysis comparing each individual variable or vulnerability was conducted using the table format function in Microsoft Xcel and the conditional formatting function. This allowed the researcher to isolate specific text within the .cve file in order to analyze the frequencies of specific variables each year. The analysis by year and by variable could not be done in QDA Miner Lite because much of the functionality is disabled in the lite version of the software. One interesting trend that was discovered while the data was being coded by flaw in Xcel was that 139 of the cases which had “cross-site scripting” in the description also had “sql” in the description. This shows that many of the vulnerabilities and exposures that have been defined are more complex than the original 41 categories defined by Christey and Martin. Out of these 139 cases which had both XSS and SQL in their description, the frequency of cases per year is noted in table 10. To provide even more clarity for reference back to the CVE List, in 2015, the 8 cases where this occurred had the following CVE List numbers: CVE-2015-1374, 3438, 3440, 4660, 5064, 6010, 6945, and 7383 (showing the last four digits only).

Table 10. XSS and SQL Flaws in the Description

Year	XSS and SQL Frequency in the Description
2001	1
2002	2
2004	6
2005	10
2006	38
2007	14
2008	16
2009	9
2010	10
2011	5
2012	6
2013	5
2014	9
2015	8

Source: Created by author.

Table 11 provides the top five most common vulnerabilities and the yearly frequency of occurrences. This analysis was conducted in Microsoft Xcel using filtering and conditional formatting on the complete .csv file. The data suggests that the five most frequent flaws go through periods of popularity among hackers. For example, in 2006 cross-site scripting and SQL injection vulnerability was highly common. Then in 2007 buffer overflows took the lead among the top five. Finally, in 2015 the “bad privilege assignment” vulnerability hit its peak and ranked third among the top five.

Table 11. Top Five Most Common Vulnerabilities by Year

RANK	TOTAL	1	2	3	4	5
FLAW		XSS	sql-inject	unk	BUF	priv
TOTAL	87883	9509	7511	7297	6326	4900
1999	1592	2	13	3	301	246
2000	1244	3	27	7	240	176
2001	1574	32	46	19	268	227
2002	2434	215	116	80	458	257
2003	1598	123	69	106	332	172
2004	2777	302	183	210	452	176
2005	4893	751	670	402	503	288
2006	7253	1332	1125	755	594	287
2007	6758	843	797	608	855	386
2008	7316	984	1574	876	603	313
2009	5149	756	733	522	581	250
2010	5324	591	655	668	410	395
2011	5330	488	195	516	423	268
2012	6700	792	334	646	388	260
2013	7446	710	279	733	373	347
2014	9659	951	374	481	297	330
2015	8785	618	299	515	291	509
2016	2068	15	22	150	11	12

Source: Created by author.

One final search term was entered into the raw data-set because of the number of times that it was mentioned in the literature review; the researcher entered "denial of service" into Xcel to count the total frequency of definitions for a denial of service attack. The total list included 15,867 cases out of 87,883 with the text "denial of service" in the description. 1,689 occurrences of the "denial of service" vulnerability were defined in 2015; 1,500 in the year 2014; and 1,493 in the year 2013. Because this was not one of the specific flaws defined by Christey and Martin it is difficult to compare this to the previous study, however it is a significantly greater number per year than the top five listed above.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

The U.S. Army Signal Corps must provide security for the Department of Defense Information Network (DODIN) by improving our security posture to withstand the threats form cyberspace and electronic warfare threats. By understanding the threats and methods used to protect against those threats the DODIN can have an improved security posture. The report from Symantec categorized threats into the following primary groups: Mobile devices and the Internet of Things, Web Threats, Social Media and Scams, Targeted Attacks, Data Breaches and Privacy, and E-Crime and Malware (Symantec 2015, 4). The Symantec report provides best practice guidelines for businesses which should be adopted or continuously used by the DoD and enforced to foster this greater security awareness within the DODIN. These best practices like employing defense-in-depth strategies, protect private keys, use encryption, and ensuring regular backups are just a few of the best practices that can show immediate improvement to the security of a network (Symantec 2014, 87-88). Continuing to foster best security practices will greatly improve the security posture of the Department of Defense Information Network.

Electronic warfare methods have been shown to include both physical threats to the network in the form of electronic attack, and logical threats to the network such as cyber-attack which occurs by unauthorized access to the network. Physical threats can come in the form of radio or radar jamming, anti-satellite weapons, or directed laser energy. Logical threats can come from cyber-attacks such as denial of service attacks, cross-site-scripting, and SQL injection. Denial of service attacks are large in number and seemingly increasing based upon the data analyzed with over 1,500 denial of service vulnerabilities defined per year in the past two years.

The literature review of previous threats to communications has provided a historical basis for the importance of a robust cyberspace and electronic warfare security strategy. Hacking attacks such as the denial of service attacks which occurred in Estonia in 2007 and Georgia in 2008 were the first indicators of a growing international threat. This prompted the creation of the Tallin Manual which provides guidelines for international laws of cyber warfare. The Stuxnet virus inflicted severe damage to Iranian nuclear infrastructure in June of 2010. Saudi Aramco fell victim to the Shamoon virus in August of 2012 which destroyed countless hard drives in the facility. In September of 2012 six U.S. banks were reportedly attacked by Iran in extreme denial of service attacks (Dev 2015, 394). Physical threats from China's development of the kinetic anti-satellite weapon have proven that it is possible to conduct precision attacks on objects in space. GPS jamming continues to be of concern, and radio jamming techniques continue to improve. All of these trends in current threats mark the increased importance of cyber protection and countermeasures for electronic warfare threats.

Examples provided from current industry standards and best practices for network security have provided an informative summary for Department of Defense leaders to reference and consider for implementation on current networks. Symantec's set of 14 best practices for businesses are just one of many valuable lessons to be learned from private industry on cyber security.

Current threats discovered by a quantitative comparison to the types of viruses and malware recorded in the Common Vulnerabilities and Exposures (CVE) List has provided a current view or threat assessment of the types of logical threats detected by the collaborative efforts of cyber security professionals. The top five threats out of the original 41 flaw types are now cross-site-scripting, SQL injection, unknown, buffer overflows, and "bad privilege assignment, or privileged process/action is unprotected/unauthenticated". Also the amount of denial of service flaw definitions per year seem to indicate that this type of flaw is increasing each year. The fact that denial of service attacks were also the reported method of attack in Georgia and Estonia support the assumption that denial of service attacks are becoming increasingly dangerous.

Recommendations

Threats against the DODIN in the form of cyber-attacks and electronic warfare will continue to evolve and increase in frequency. Monitoring trends and continuing education on network protection and cyber security will continue to play an important role for U.S. Army Signal Officers. Leaders must study reports from current cyber-attacks and understand how to implement protections against electronic warfare measures. Leaders must be prepared to provide electronic warfare protection in the physical domain and cybersecurity in the logical domain. Studying the analysis by year and by variable could not be done in QDA Miner Lite because many of the functionality is disabled in the lite version of the software. Future research using more text analysis of the flaw descriptions could help to identify other trends in the vulnerabilities defined each year. Continuous monitoring of evolving cyber-security threats must occur. By understanding the cyber and electronic warfare threats, leaders can prepare to employ appropriate countermeasures in or to ensure continued operations of the Department of Defense Information Networks (DODIN).

REFERENCE LIST

ARCIC. 2016. “Army Warfighting Challenges.” Accessed January 17, 2016. http://www.arcic.army.mil/Initiatives/army-warfighting-challenges.aspx.

Bussing, Joseph. 2013. “The Degrees of Force Exercised in the Cyber Battlespace.” *Connections: The Quarterly Journal* 12, no. 4: 1-13. Accessed January 17, 2016. https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/1501475997?accountid=28992.

Carter, Ash. 2015. “The DoD Cyber Strategy.” *Defense News*. Accessed May 9, 2016. http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.

Christey, Steve, and Robert A. Martin. 2007. “Vulnerability Type Distributions in CVE.” Accessed January 17, 2016. https://cve.mitre.org/cve/identifiers/index.html.

Creswell, John W. 2003. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 2nd ed. Los Angeles, CA: Sage Publications.

———. 2007. *Qualitative Enquiry and Research Design: Choosing Among Five Approaches*. Los Angeles, CA: Sage Publications.

———. 2013. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Los Angeles, CA: Sage publications.

CVE. 2016. “About CVE Identifiers.” Accessed January 17, 2016. https://cve.mitre.org/cve/identifiers/index.html.

Daugirdas, Kristina, and Julian Davis Mortenson. 2015. “United States Responds to Alleged North Korean Cyber Attack on Sony Pictures Entertainment.” *American Journal of International Law* 109, no. 2: 419-422.

Department of the Army. 2016. ATP 6-02.53, *Techniques for Tactical Radio Operations*. Washington, DC: Department of the Army.

Dev, Priyanka R. 2015. “’Use of Force’ and ‘Armed Attack’ Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response.” *Texas International Law Journal* 50, no. 2: 381-401. Accessed January 17, 2016. https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/1704865288?accountid=28992.

Forden, Geoffrey. 2007. “After China's Test: Time For a Limited Ban on Anti-Satellite Weapons.” *Arms Control Today* 37, no. 3: 19-23. Accessed May 9, 2016. http://search.proquest.com.lumen.cgsccarl.com/docview/211282478?accountid=28992.

Gould, Joe. 2015. “Electronic Warfare: What US Army Can Learn from Ukraine.” *Defense News*, 4 August 2015. . Accessed May 9, 2016. http://www.defensenews.com/story/defense/policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397/.

Gordon IV, John, and John Matsumura. 2013. *The Army's Role in Overcoming Anti-Access and Area Denial Challenges*. Santa Monica, CA: RAND.

Graham, Adrian. 2011. *Communications, Radar and Electronic Warfare*. Hoboken, NJ: John Wiley and Sons.

Grego, Laura. 2012. “A History of Anti-Satellite Programs.” Union of Concerned Scientists, January, 1-16. Accessed November 7, 2015. http://www.ucsusa.org/nuclear-weapons/space-security/a-history-of-anti-satellite-programs#.Vkv-bvmrSUk.

Haggard, Stephan, and Jon R. Lindsay. 2015. “North Korea and the Sony Hack: Exporting Instability Through Cyberspace.” *Asiapacific* no. 117: 1-8. Academic Search Complete, EBSCOhost. Accessed November 7, 2015.

Herzog, Stephen. 2011. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security* 4, no. 2: 49.

House, Garvey. 2014. *PhD Dissertation Guidebook: School of Business and Technology*. Minneapolis, MN, Capella University.

Kramer, David J. 2015. “The Ukraine Invasion.” *World Affairs* 177, no. 6: 9-16. Military and Government Collection, EBSCOhost. Accessed January 17, 2016.

Korns, Stephen W., and Joshua E. Kastenberg. 2009. “Georgia's Cyber Left Hook.” *Parameters* 38, no. 4: 60-76. Accessed January 17, 2016. https://lumen.cgsccarl.com/login?url=http://search.proquest.com.lumen.cgsccarl.com/docview/198032208?accountid=28992.

Lungerman, Joseph. 2014. “What Happens if They Say No?” *Air and Space Power Journal* (November-December): 103-116. Accessed November 7, 2015. http://www.airpower.au.af.mil/article.asp?id=239.

Martin, Robert A. 2008. “Making Security Measurable and Manageable.” Military Communications Conference. MILCOM, IEEE.

MITRE. 2016. “Common Vulnerabilities and Exposures.” MITRE website. Accessed January 17, 2016. https://cve.mitre.org/.

Mpitziopoulos, Aristides, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou. 2009. “A Survey on Jamming Attacks and Countermeasures in WSNs.” *IEEE Communications Surveys and Tutorials* 11, no. 4: 42-56.

Nakashima, Ellen. 2015. “Chinese Hack Compromised Security-Clearance Database.” *The Washington Post*, June 12. Accessed January 17, 2016. http://search.proquest.com.lumen.cgsccarl.com/docview/1687796487?accountid=28992.

Neuhaus, Stephan, and Thomas Zimmermann. 2010. “Security Trend Analysis with CVE Topic Models.” IEEE 21st international symposium.

Pagilery, Jose. 2014. “’Sony-pocalypse’: Why the Sony Hack is one of the Worst Hacks Ever.” *CNN Money*, December 4. Accessed November 7, 2015. http://money.cnn.com/2014/12/04/technology/security/sony-hack/?iid=EL.

———. 2015. “The Inside Story of the Biggest Hack in History.” *CNN Money*, August 5. Accessed November 7, 2015. http://money.cnn.com/2015/08/05/technology/aramco-hack/.

Pallin, Carolina Vendil, and Fredrik Westerlund. 2009. “Russia's War in Georgia: Lessons and Consequences.” *Small Wars and Insurgencies* 20, no. 2: 400-424. Accessed November 17, 2015. http://dx.doi.org/10.1080/09592310902975539.

Pandit, Rajat. 2012. “After Agni-V launch, DRDO’s New Target is Anti-Satellite Weapons.” *The Times of India*. Accessed May 9, 2016. http://timesofindia.indiatimes.com/india/After-Agni-V-launch-DRDOs-new-target-is-anti-satellite-weapons/articleshow/12763074.cms.

Perlroth, Nicole. 2012a. “In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back.” *The New York Times*, October 23. Accessed November 7, 2015. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0.

———. 2012b. “Attacks on 6 Banks Frustrate Customers.” *The New York Times*, October 1. Accessed November 7, 2015. http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html?_r=0.

Pifer, Steven. 2015. “Russian Aggression against Ukraine, and the West's Policy Response.” *Hampton Roads International Security Quarterly*: 23. Accessed May 9, 2016. http://search.proquest.com.lumen.cgsccarl.com/docview/1669501431?accountid=28992.

Rossiyskaya Gazeta. 2015. “Russia's Electronic Warfare Systems Ensure “A2/AD.” BBC Monitoring Former Soviet Union. Accessed November 7, 2015. http://search.proquest.com.lumen.cgsccarl.com/docview/1729772684?accountid=28992.

Schmitt, Michael N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York, NY: Cambridge University Press.

Segodnya, Rossiya. 2015 “Russia's Largest Electronic Warfare Company Developing Spacecraft Equipment.” BBC Monitoring Former Soviet Union, May 6. Accessed May 9, 2016. http://search.proquest.com.lumen.cgsccarl.com/docview/1678722017?accountid=28992.

Shahani, Aarti. 2015. “Report: To Aid Combat, Russia Wages Cyberwar against Ukraine.” NPR All Tech Considered, April 28. Accessed November 7, 2015. http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine.

Symantec. 2014. Internet Security Threat Report Volume 19. Accessed May 9, 2016. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

———. 2015. Internet Security Threat Report Volume 20. Accessed May 9, 2016. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

Turabian, Kate L. 2013. *A Manual for Writers of Term Papers, Theses, and Dissertations.* 8th ed., Rev. Ed. Wayne C. Booth, Gregory G. Colomb, Joseph M. Williams, and the University of Chicago Press Editorial Staff. Chicago: University of Chicago Press.

U.S. Army. Command and General Staff College. 2014. ST 20-10, *Master of Military Art And Science (MMAS) Research and Thesis.* Ft. Leavenworth, KS: USA CGSC, August.

Wang, Ju An, Minzhe Guo, Hao Wang, and Linfeng Zhou. 2012. “Measuring and ranking attacks based on vulnerability analysis.” *Information Systems and e-Business Management* 10, no. 4, 455-490.

Wiser, Daniel. 2015. *How Russia Invaded Ukraine*. The Washington Free Beacon, 18 September. Accessed May 9, 2016. http://freebeacon.com/national-security/how-russia-invaded-ukraine/.